Express5800/320Lc
System Release Notes

PN: 455-01816-000

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of NEC Solutions (America), Inc. and/or its licensors. NEC Solutions (America), Inc. and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The NEC Solutions (America), Inc. product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by NEC Solutions (America), Inc.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC Solutions (America), Inc. is prohibited.

Trademarks

Microsoft and Windows 2003 are registered trademarks of Microsoft Corporation.

PROSet II is a registered trademark of Intel Corporation

VERITAS is a registered trademark of VERITAS Software Corporation

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

PN: 455-01816-000 February 2005

Copyright 2005
NEC Solutions (America), Inc
10850 Gold Center Drive, Suite 200,
Rancho Cordova, CA 95670
All Rights Reserved

Express5800/320Lc
System Release Notes

The *Express5800/320Lc System Release Notes* provide up-to-date information on your system. These notes also provide additional valuable information about your system that was not included in the user's guide at the time of its release.

Please read these notes in their entirety.

CONTENTS

Introduction 2
Operating System 2
Advisories 2
  EXPRESSBUILDER 2
  System Hardware 2
  Windows Server 2003 4
  Other System Software 4
Precautions 5
Notes 15

Introduction

These System Release Notes cover the following topics:

- Operating System
- Advisories
- Precautions
- Notes

Operating System

The following general comments apply to this server.

- Versions of the Network Operating Systems tested and recommended are:

  — Microsoft Windows® 2003 Enterprise Edition.

- Microsoft Windows® 2000, NT© 4.0, and FT Linux are not supported.

Advisories

EXPRESSBUILDER

The following advisory applies to EXPRESSBUILDER.

- Install the Windows Operating System using the Ft Server Setup function on EXPRESSBUILDER. Do not attempt to install the operating system manually.
- The version of EXPRESSBUILDER is specific to the operating system supported. The appropriate EXPRESSBUILDER is shipped for the configured operating system. If an operating system is not configured, use the EXPRESSBUIDER appropriate for your installation.
  - EXPRESSBUILDER 3.011 versions support Windows Server 2003 Enterprise Edition.

System Hardware

The following advisories apply to system hardware.

- SCSI disk LED's are green when the OS is rebooting.
- When a PCI module is removed, the disk LED's for the disks in the active PCI module are off.
- After a PCI module failover, the drive letter of the USB floppy drive changes. If the floppy drive letter is A:, it changes to B: If the floppy drive letter is B:, it changes to A:.
- OS installation must be performed with only one hard disk drive installed in slot #1 of PCI module #1. Otherwise, the keyboard, mouse and additional hard disk drives may not be recognized.

- Do not perform Device Manager "Scan for Hardware Changes" while performing a backup, otherwise the backup may fail.
- The keyboard and mouse may not respond during a BIOS online update. Once the BIOS is completely updated, keyboard/mouse functionality is restored.
  - When removing the USB diskette drive from the system, use “Add/ Remove Hardware” in the Control Panel. If the USB diskette drive is not cleanly removed, the keyboard and/or mouse may not respond. If the keyboard and/or mouse no longer respond, remove the USB keyboard from the system and reconnect it. Keyboard and mouse functionality will be restored.
  - When the system is connected to a UPS for planned shutdowns and reboots, it is possible that the active PCI module and the active Power Switch LED will switch between modules. This is due to slight timing differences in the boot sequences and may cause a different PCI module to be considered “primary” each time the system is power cycled.
  - When adding a new (i.e.. no operating system signature) hard disk drive to the system, add the hard disk drive while the operating system is up and running. If the new hard disk drive is introduced into the system when the system is not at the operating system level, the PCI modules may not duplex. If such a condition occurs, remove the new disk and re-insert it. The disk will be recognized and the PCI modules will duplex.
  - Determining a defective disk (i.e.. ascertaining the physical location), requires the following information.
    - **Port Number:** The port number can be determined from ESMPRO's DataViewer. SCSI Enclosure (ID:10/40/120) for PCI module #1 and SCSI Enclosure (ID:11/40/120) for PCI module #2.
    - **Target Number:** The Target Number can be determined from VERITAS Enterprise Administrator Check each disks' Properties. Each disk will have a Port Number and a Target Number. The Port Number will correspond with the PCI module determined in above under Port Number. The Target Number corresponds as follows:

Target	Disk Slot
0	1
1	2
2	3

- If you have computers that communicate with the EXPRESS5800/320Lc Series server using TCP/IP protocols, you must make several configuration settings to the server to allow communications without interruptions. These TCP/IP configuration settings must also be made to all systems connected to the EXPRESS5800/320Lc server via the network. For other operating systems, consult your operating system documentation to determine the equivalent procedure(s).
  - The selection of a PXE boot device in the BIOS Setup Utility Boot Menu is not currently supported on Express5800/320Lc/320Lc-R.
  - The high availability server allows you to remove, install, and replace the following devices while the server is in continuous operation:
    - CPU Module
    - PCI Module
    - Disk Drives
  - A system reboot is required when the following components are installed:
    - CPUs
    - DIMMs
    - PCI option cards
  - The Express5800/320Lc(320Lc-R) may appear to hang with a blank screen when shutting down prior to a restart. This behavior has typically been noted when a USB to PS2 converter is used for the mouse and/or keyboard, with or without a KVM switch. As a workaround for this situation, remove and replace the keyboard/mouse USB cable in the USB port. System operation should continue after the cable is removed.

Windows Server 2003

The following advisories apply to Windows Server 2003.

- Veritas Volume Manager is not supported with the Windows Server 2003 operating system.

Other System Software

The following advisories apply to system software.

- Intel PROSet© II must be removed then re-installed whenever all the LAN adapter teams have been removed. The LAN adapter teams must be re-created after Intel PROSet is re-installed.
- The Windows System Event Log may show SCSI controller errors containing "f0030015" in the last data word while backup software is running. These errors may be ignored.

- When backup software is installed and a PCI module needs to be serviced, terminate the backup software service before replacing PCI modules.

Precautions

The following are precautions and limitations of the ft control software Version 3.0 for the Express5800/320Lc/Lc-R. Please read the list of notices below carefully to ensure that they are followed.

1. Precautions for relocating the Server

When relocating the server after setup, there is a possibility that some connectors which connect the back panel and each module becomes broken due to shock or vibration caused by transportation or inappropriate packing. This could cause a fatal problem to the server. Please read the following, if you need/plan to relocate the server after setup:

a) If you perform pre-setup to the server at a temporary place, keep the packaging box and reuse it when relocating the server.

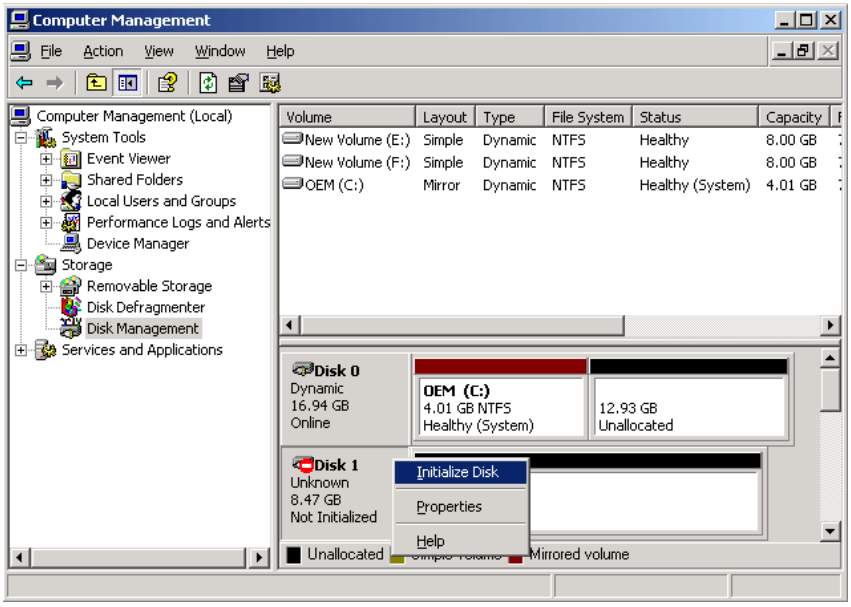
b) When relocating or transporting, remove all module from the main chassis and pack each module. This does not mean that you need to prepare boxes for each module. One box may contain one or more modules. If you plan to relocate the server later, it is recommended that you keep the packaging box and reuse it when relocating the server.

c) If you relocate a 320Lc-R (rack-mount model), remove all modules from the main chassis before moving the main chassis. Even when relocating the server without packing (e.g. by a hand cart), remove all modules from the main chassis before moving the main chassis.

2. Precautions when adding HDD

When an unused HDD (no signature) is added, in rare instances, the redundancy of the PCI modules will become failed. (Status LED2 of the PCI module in which the HDD was added, will be lit amber.)

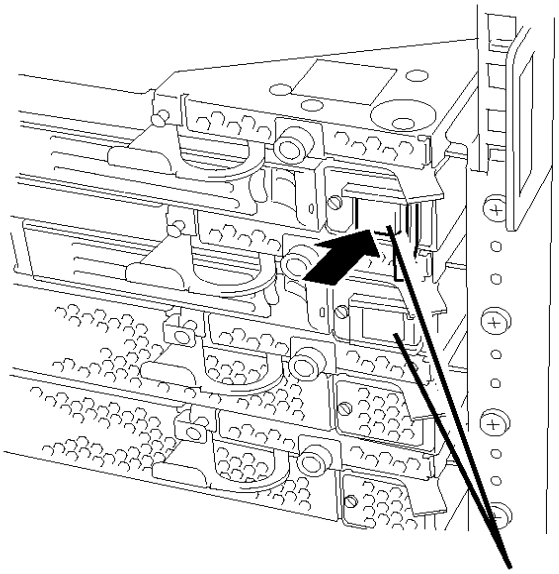
When status LED2 of the PCI module in which the HDD was added is lit amber, the problem can be rectified using [Disk Management] from [Computer Management] (My Computer → Properties). Initialize the newly added HDD, by right clicking the HDD, and click [Initialize Disk]. After the initialization, duplication of the PCI modules should commence, and the status LED2 of the PCI module will become green.



Note: Disk signature as mentioned above, refers to the signature that is written to the hard disk, which allows for its use on the Windows operating system.

3. POWER switch lamp during auto-operation with UPS

When a UPS regulates the power supply of the server automatically, the POWER switch, which becomes lit, may differ from before shutdown. This is due to the AC ON timing of each module. This will not affect any functions or any operations of the NEC Express5800/ft series system.



POWER switch (including POWER lamp)

4. Notice when using backup application software

Do not perform "Scan for hardware changes" in the device manager while performing backup. The backup job may fail if hardware is scanned during the backup process.

5. Connection of 8-port server switch unit (SSU)

Mouse devices and keyboards of other computers connected to the 8-port SSU may stop responding while the NEC Express5800/ft series server boots or shuts down.

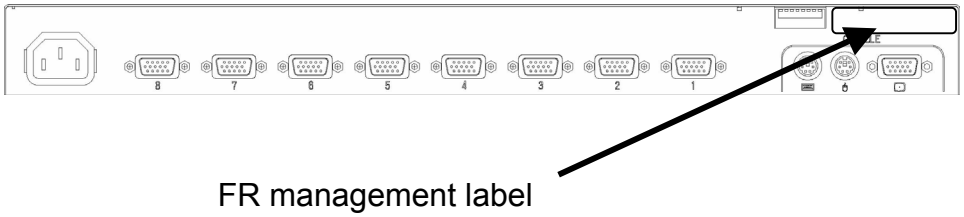
After the NEC Express5800/ft series server is powered up completely, mouse devices and keyboards will work properly, please wait for approximately 30 sec. in such a case.

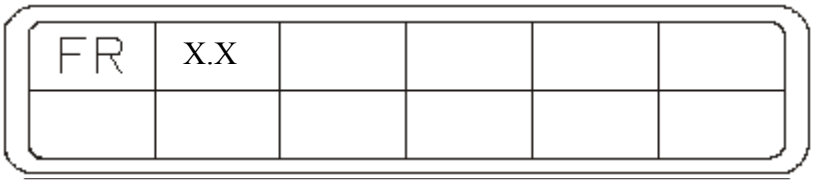
> ***Note:*** This problem may occur if the FR management number of the 8-port SSU is 1.2 or earlier. This problem will not occur on devices where the FR management number is 1.3 or later.

The FR management number is written on the FR management label. (See below).

Location of FR management label

Back of 8 port server switch unit





If there is more then one set of numbers on the FR management label, the largest number that appears will be the current FR management number.

6. Cautions when running on-line update of the system BIOS

The mouse and keyboard may stop responding temporarily when running the on-line system BIOS update from the “ft server utility”, or the “NEC ESMPRO Manager”. They will automatically be restored after the updating of the system BIOS is completed.

7. Cautions regarding status lamps of the PCI modules during HDD failure

When a failure of an internal HDD of the PCI module occurs, in some instances, the status lamps of both PCI modules will turn amber, and the duplication of the modules will become broken.

In such an occurrence, exchanging the failed HDD, and re-mirroring the HDD can rectify the problem. Status lamp2 of the PCI modules will change to green, and the duplication of the modules will be enabled.

Refer to the User’s Guide for details of each process.

* Refer to the following chapters of the User’s Guide regarding how to identify the faulty HDD.
    1) [2 General Description]-[NAMES AND FUNCTIONS OF COMPONENTS]-[LEDs]-[Hard Disk LED]
    2) [3 Windows Setup and Operation]-[DISK OPERATIONS]-[Replacing Failed Hard Disk Drives]-[How to Locate Failed Disks]
* Refer to the following chapter of the User’s Guide regarding the re-mirroring. procedure.
    1) [3 Windows Setup and Operation]-[DISK OPERATIONS]-[Replacing Failed Hard Disk Drives]-[Procedures to Replace Failed Disks]

8. Notes during BMC FW update service

The following error event may be recorded in the system log if the system is the amount of load is relatively high.

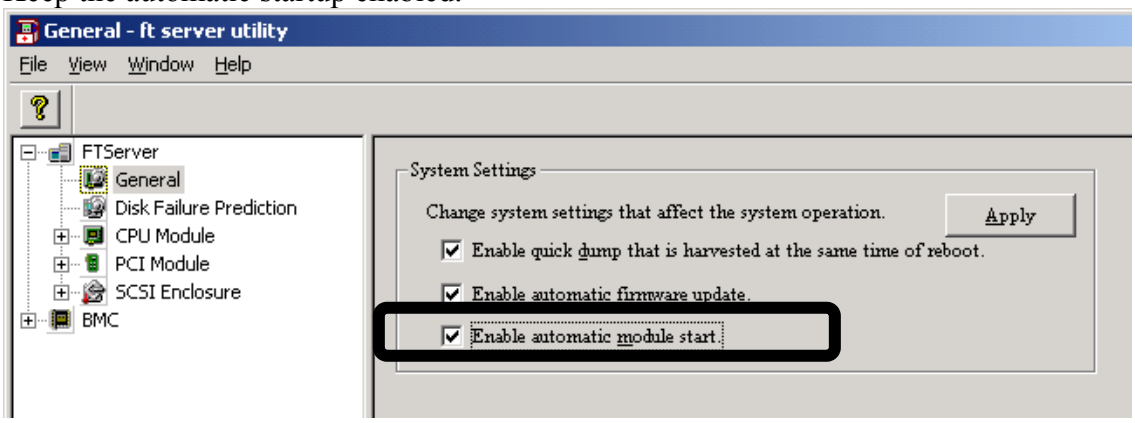
Source:BMC FW Update Service
Event ID:1
Description: Illegal data file.
The "bmcfg.inf" file is illegal.
(Error Code. = 81)

This event log is outputted if the update data is not specified properly when BMC firmware update is performed from NEC ESMPRO Manager or ft server utility. However, in rare instances, it is outputted improperly when the amount of load is relatively high.
If this event log is outputted when BMC firmware update is not performed, ignore it since the system has no problem.

9. Cautions regarding [Enable automatic module start.] option in the ft server utility

The duplication of the PCI modules may not be performed properly if the automatic startup is disabled by unchecking [General]-[System Settings]-[Enable automatic module start.] option in the ft server utility. Especially when the optional boards are installed.

Keep the automatic startup enabled.



Note: Do not uncheck this item.

If the PCI module maintenance is performed in the environment where this item is unchecked, the PCI module may not be duplicated properly. In that case, please follow the steps shown below.

1. Check [Enable automatic module start.] in the ft server utility and click Apply].
2. When the HDD has been mirrored, open the ft server utility and stop the PCI module of which status LED 2 is lit in green.
3. Remove the stopped PCI module once, and insert it back after waiting a little.
4. After the HDD mirroring has been completed, the status LED2 on both PCI modules will light in green, and the PCI module will be successfully duplicated.

10. Cautions for removing the RDR setting of the HDD, which has been mirrored with RDR

When the RDR setting is removed from one of the HDD, which has been mirrored with RDR, and the HDD does not have any partitions, the status LED2 of the PCI module, which has the removed HDD, may light in amber, and show the non-duplicated status.

When this status appears, follow the steps show below and restore the proper status.

1) Start the [Start]-[Administrative Tools]-[Services].
2) Right-click on the Stratus ftServer Storage Manager, and execute Restart.

> ***Note:*** This caution applies only to 320Lc/Lc-R with Rapid Disk Resync.

11. Cautions for the system booted

In a very rare case, the duplications of the CPU/PCI modules stop when the server which “ft control software Ver.3.0 Update module No.001 FD” is not applied is started.

Usually, it is recovered automatically at stop of the duplications because the update module for this phenomenon is applicable when the server is set up Event logs 1,2,3 are registered.

Please recover after applying the update module referring to “Procedure to recover” because the system becomes the following in case of un-application.

<Status of the duplications stopped>
-Status of Status LED

Module	Status LEDs(1 and 2)
PCI module Group 1	Green / Red
PCI module Group 2	Green / Red
CPU module 1	off / Amber
CPU module 2	Red / off

> ***Note:*** If the duplication stops when the system is rebooted, the status LED (1 and 2) of both CPU modules will be off / Green.

Please check the following information also, as the LED status show above may vary depending on when the duplication stops.

-Event log
Start [Start]-[Administrative Tools]-[Event Viewer], and select the system in the left pane, and confirm that the following logs are registered.

1. Event Source: Service Control Manager
   Event ID: 7022

Description: The Stratus ftServer Provider Manager service hung on starting.

2. Event Source: Service Control Manager
   Event ID: 7022
   Description: The Stratus ftServer Storage Manager service hung on starting.

3. Event Source: Service Control Manager
   Event ID: 7031
   Description: The Stratus ftServer Maintenance and Diagnostics (MAD) service terminated unexpectedly. It has done this 3 time(s). The following corrective action will be taken in 0 milliseconds: Run the configured recovery program.

4. Event Source: Service Control Manager
   Event ID: 7032
   Description: The Service Control Manager tried to take a corrective action (Run the configured recovery program) after the unexpected termination of the Stratus ftServer Maintenance and Diagnostics (MAD) service, but this action failed with the following error:
   The system cannot find the file specified.

-Services
Start [Start]-[Administrative Tools]-[Services].
Confirm the status of the following services.

Name	Status
Stratus ftServer Maintenance and Diagnostics(MAD)	
Stratus ftServer Provider Manager	starting
Stratus ftServer Storage Manager	starting

If the all status are same as above and the duplication of the modules has been stopped, follow the steps shown below to restart the duplication.

<Procedure to recover>

1. Apply “ft control software Ver.3.0 Update module No.001 FD” referring to “Step 7: Update Software” of User’s Guide (Setup).
2. Confirm that it has been applied normally seeing “Procedure to confirm update module application”.
3. Perform “recovery.bat” in C:\ProgramFiles\Stratus\Utility(when a system drive is “C”).
   After the steps show above has finished, the duplication of each module will be restarted.

<Procedure to confirm update module application>

- Confirm dependencies of services

1. Start [Start]-[Administrative Tools]-[Services], and right-click the following services and display properties.
   - Stratus ftServer Maintenance and Diagnostics(MAD)
   - Stratus ftServer Provider Manager
   - Stratus ftServer Storage Manager
2. Select “Dependencies” tab, and confirm the following components are added on “This service depends on the following system components”.
   - Plug and Play
   - Remote Procedure Call (RPC)
   - Windows Management Instrumentation

- Confirm recovery program of service

1. Start [Start]-[Administrative Tools]-[Services], and right-click the following service and display properties.
   - Stratus ftServer Maintenance and Diagnostics(MAD)
2. Select “Recovery” tab, and confirm that the following path is set on “Program”.
   C:\ProgramFiles\Stratus\Utility\recovery.bat
   (when a system drive is “C”)

12. Cautions for using the Windows Server 2003 Recovery Console

Windows Server 2003 Recovery Console cannot execute the copy command to the following hard disk. “Access is denied” message will appear.

Dynamic disk

When you are executing the copy command to the disk shown above in the Windows Server 2003 Recovery Console, you must make the following setting.

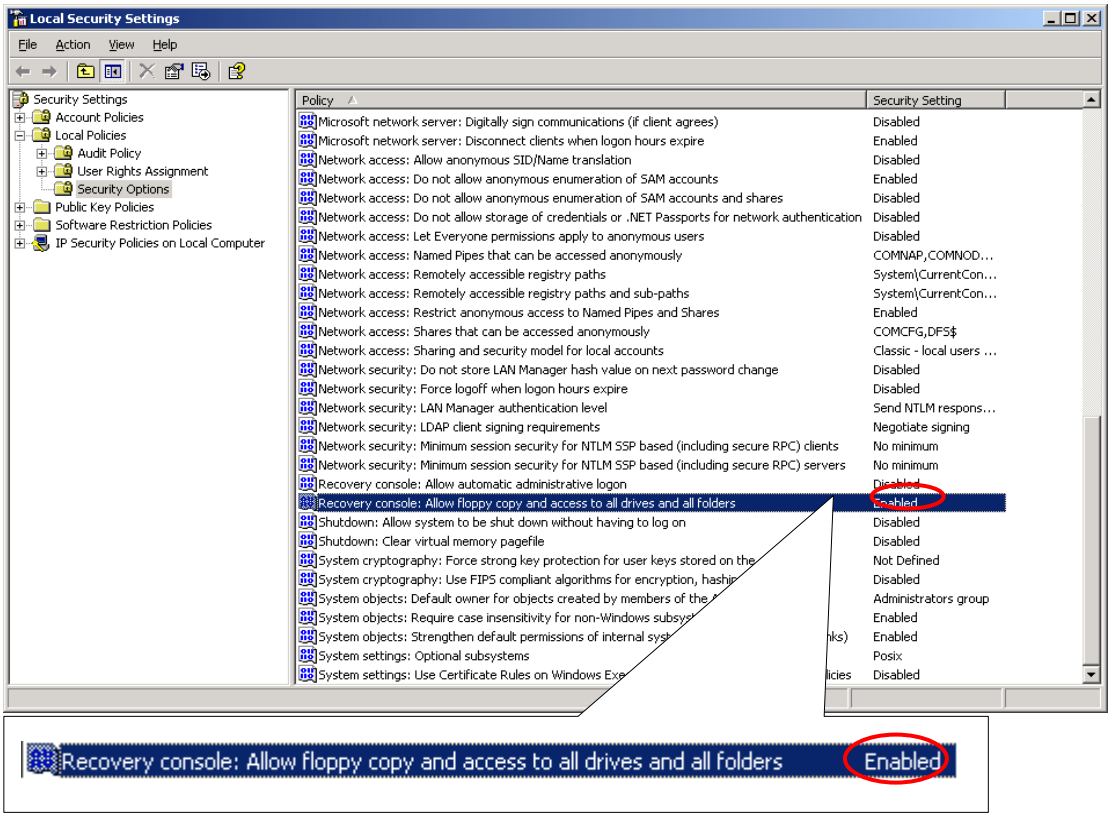
> **Note:** The copy command can be executed to the basic disk.

[Setting]

1) [Local Security Policy] setting

Note)
This setting should be made on the Windows Server 2003 in advance.

1. Start Windows Server 2003, and log on as a user with the administrator authority.
2. Start [Start]-[Administrative Tools]-[Local Security Policy].
3. Select the [Local Policies]-[Security Options] from the left window of the [Local Security Settings] screen.
4. Double-click on [Recovery console: Allow floppy copy and access to all drives and all folders] in the right window, and enable the Security Setting.


Local Security Settings
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Policy
Security Setting
Microsoft network server: Digitally sign communications (if client agrees) Disabled
Microsoft network server: Disconnect clients when logon hours expire Enabled
Network access: Allow anonymous SID/Name translation Disabled
Network access: Do not allow anonymous enumeration of SAM accounts Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares Disabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication Disabled
Network access: Let Everyone permissions apply to anonymous users Disabled
Network access: Named Pipes that can be accessed anonymously COMNAP,COMNOD...
Network access: Remotely accessible registry paths System\CurrentCon...
Network access: Remotely accessible registry paths and sub-paths System\CurrentCon...
Network access: Restrict anonymous access to Named Pipes and Shares Enabled
Network access: Shares that can be accessed anonymously COMCFG,DFS$
Network access: Sharing and security model for local accounts Classic - local users ...
Network security: Do not store LAN Manager hash value on next password change Disabled
Network security: Force logoff when logon hours expire Disabled
Network security: LAN Manager authentication level Send NTLM respons...
Network security: LDAP client signing requirements Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers No minimum
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives and all folders Enabled
Shutdown: Allow system to be shut down without having to log on Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Force strong key protection for user keys stored on the Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashi Disabled
System objects: Default owner for objects created by members of the Administrators group
System objects: Require case insensitivity for non-Windows subsys Enabled
System objects: Strengthen default permissions of internal sys Enabled
System settings: Optional subsystems Posix
System settings: Use Certificate Rules on Windows Exe Disabled
Recovery console: Allow floppy copy and access to all drives and all folders Enabled

2) Environment variable “AllowRemovableMedia” setting

Note)

This setting is made on the Windows Server 2003 Recovery Console when the Windows Server 2003 Recovery Console is in use.

This should be set everytime when the Recovery Console is started.

1. Start the Windows Server 2003 Recovery Console

Regarding how to start the Recovery Console, refer to the following chapters in the User’s Guide(Setup)

[TROUBLESHOOTING]-[System Repair] following chapters.

[Preparation]

[Starting up Recovery Console]

2. Log on to the Recovery Console, and execute the following command. (The default is FALSE)

set AllowRemovableMedia = TRUE

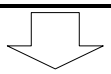
Remarks)

The copy command can be executed to the dynamic disk on the Windows Server 2003 Recovery Console after the setting shown above is made.

As the default, the Windows Server 2003 Recovery Console is not allowed to execute the copy from the basic/dynamic disk to a floppy disk. However, after the setting shown above is made, the copy command can be executed to a floppy disk.

Default setting

Copy command		Basic disk	Dynamic disk
Copy From	Copy To		
HDD	→ HDD	Copy available	Copy not available
FD	→ HDD	Copy available	Copy not available
CD	→ HDD	Copy available	Copy not available
CD	→ FD	Copy not available	Copy not available
HDD	→ FD	Copy not available	Copy not available



After the setting

Copy command		Basic disk	Dynamic disk
Copy From	Copy To		
HDD	→ HDD	Copy available	Copy available
FD	→ HDD	Copy available	Copy available
CD	→ HDD	Copy available	Copy available
CD	→ FD	Copy available	Copy available
HDD	→ FD	Copy available	Copy available

HDD : Hard disk (SystemDrive,, SystemRoot only)
FD : Floppy disk
CD : CD-ROM

13. The abnormal status of the PCI module status LED

If BMC firmware is updated by BMC firmware update utility, the PCI module status LED 1/2 and BMC status LED may not light correctly even if the update has been completed properly. (The LED status may not return to the previous status after BMC firmware update.)

Normal/Abnormal status of Status LED

		Normal	Abnormal
Primary PCI module			
	BMC status LED	Green	Green or Off
	PCI module status LED 1	Off	Red
	PCI module status LED 2	Green	Off
Secondary PCI module			
	BMC status LED	Off	Off
	PCI module status LED 1	Off	Off
	PCI module status LED 2	Green	Green

If the LEDs are in such abnormal status, follow the steps shown below to restart “Stratus ftServer Maintenance and Diagnostics (MAD)” service for the recovery.

1. Click on [Start]-[Administrative Tools]-[Services].
2. Right-click on [Stratus ftServer Maintenance and Diagnostics (MAD)] in the right pane of the displayed dialog.
3. Select [Restart] from the displayed menu, and restart the service.

Also, in case that the LEDs become abnormal in the system running, follow the above procedures and confirm that the LEDs light correctly.

Notes

The following are notes for errors during system boot. Please read the notes carefully to ensure that they are followed, if error occurs.

- **If STOP error occurs**

  If a message "STOP:0x0000007B INACCESSIBLE_BOOT_DEVICE" is displayed and the system cannot boot properly, the Boot Monitoring function (Boot Monitoring Time-out Period) works and it then tries to reboot changing the boot pair (combination of CPU module and PCI module).

  This function makes it possible that the system can reboot with the other mirrored DISK when the above "STOP error" possibly caused by temporary errors on the primary DISK occurs.

  Therefore, please wait for the boot monitoring time-out period (10 minutes as default), if you see this error.

> ***Note:*** Please refer to the Boot Pair Change Sequence example, Figure 1, on page 16.

- **If an error occurs during POST**

  If the system stalls during POST, please wait until the Boot monitoring timer detects time-out and changes the boot pair as well.

  If the error occurs again during the reboot even with the changed boot pair, please contact your sales representative.

Common Notices

1) Boot Monitoring setting must be enabled.

> ***Note:*** Please refer to "Monitoring Configuration" in User's Guide for details on the Boot Monitoring function.

2) If you have the system schedule-operated, take the start time of applications and Boot Monitoring Time-out Period into consideration.

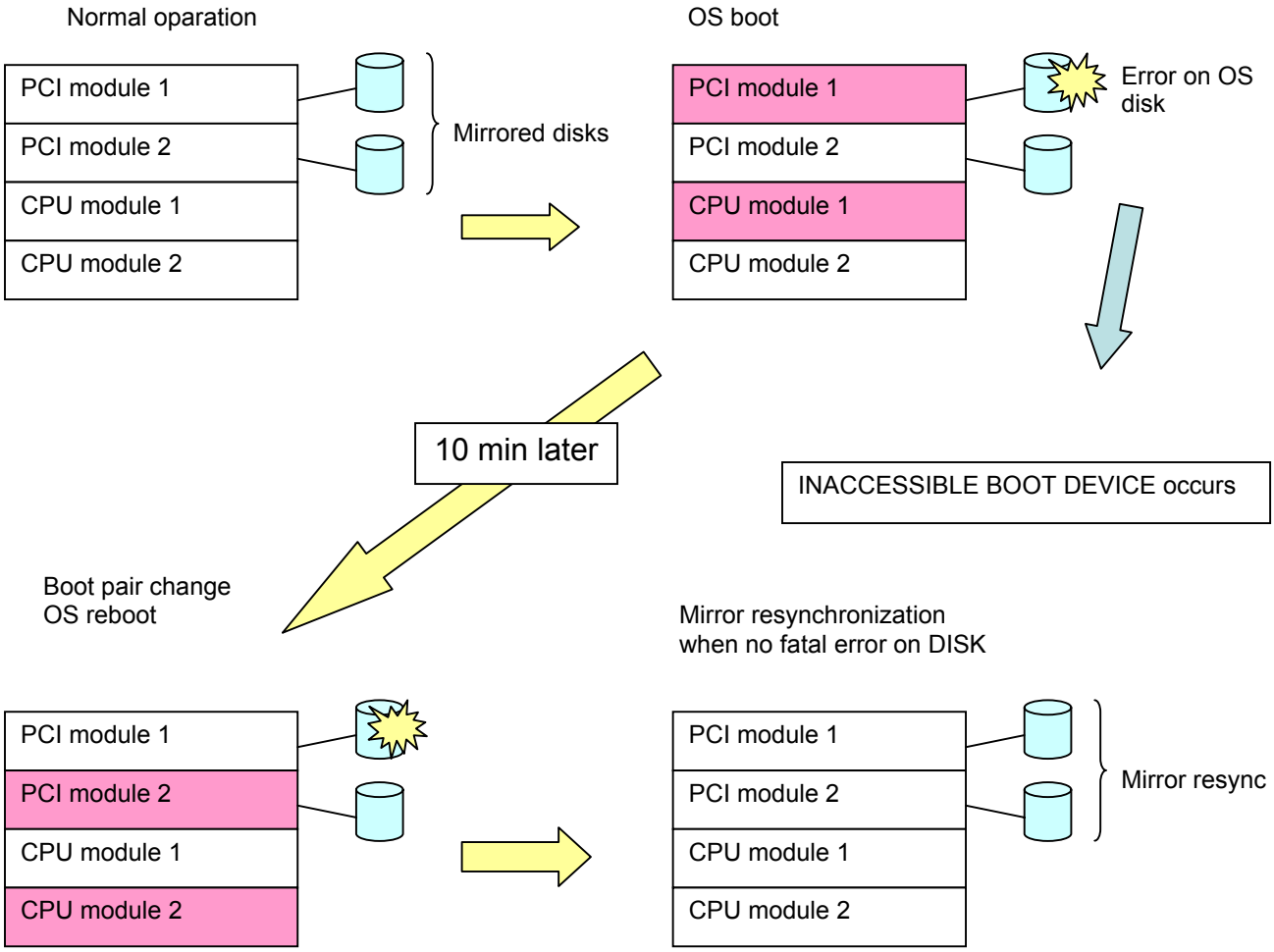


Figure 1. Image of boot pair change (example)

Selected module as primary module